

**Department of Energy**  
**Privacy Impact Assessment (PIA)**

**Name of Project:** *NGP Fellow Application System*  
**Bureau:** *Department of Energy (DOE)*  
**Project Unique ID:**  
**Date:** 05/12/2008

**A. CONTACT INFORMATION**

**1. Who is the person completing this document?**

*Olavi Aho*  
*Pacific Northwest National Laboratory*  
*Software Developer*  
*PO Box 999*  
*MS: K7-22*  
*Richland, WA 99352*  
*Olavi.aho@pnl.gov*

**2. Who is the system owner?**

*Jana Fankhauser*  
*Pacific Northwest National Laboratory*  
*Global Security Tech & Policy*  
*Project Manager*  
*1100 Dexter Ave N. Suite 400*  
*BSRC*  
*Seattle, WA 98109-3598*  
*(206) 528-3264*  
*Jana.fanhauser@pnl.gov*

**3. Who is the system manager for this system or application?**

*Jana Fankhauser*  
*Pacific Northwest National Laboratory*  
*Global Security Tech & Policy*  
*Project Manager*  
*1100 Dexter Ave N. Suite 400*  
*BSRC*  
*Seattle, WA 98109-3598*  
*(206) 528-3264*  
*Jana.fanhauser@pnl.gov*

**4. Who is the IT Security Manager who reviewed this document?**

*Shannon Mace*  
*Security Specialist*  
*Battelle, Pacific Northwest National Laboratory*  
*509-375-6968*

*Shannon.mace@pnl.gov*

**5. Who is the Privacy Act Officer who reviewed this document?**

*Mike Talbot  
Pacific Northwest Site Office  
509-372-4365  
Michael.talbot@pnl.gov*

**B. SYSTEM APPLICATION/GENERAL INFORMATION**

**1. Does this system contain any information about individuals?**

The following information will be collected from the user:

1. Full Name
2. If the applicant holds a dual citizenship, and to what countries.
3. Birth city, state and country.
4. Current and permanent address.
5. Primary and alternate email address(es)
6. Emergency contact name, address, and phone number(s)
7. Letter of interest when applying to the NGP program.
8. A current resume, text.
9. SF86 Form data.
10. Information from last six universities, including the following information:
  - a. University name
  - b. Location
  - c. Dates attended
  - d. Academic Major and Minor
  - e. Academic Status
  - f. Degree sought/obtained
  - g. Date degree received.
11. Transcripts provided by each university (scanned / uploaded at a later date)

**a. Is this information identifiable to the individual? <sup>1</sup>**

---

<sup>1</sup> "Identifiable Form" - According to the OMB Memo M-02-22, this means information in an IT system or online collection: (i) that directly identifies an individual (e.g., name, address, social security number or other identifying number or code, telephone number, email address, etc.) or (ii) by which an agency intends to identify specific individuals in conjunction with other data elements, i.e., indirect identification. (These data elements may include a combination of gender, race, birth date, geographic indicator, and other descriptor).

Yes.

**b. Is the information about individual members of the public?**

Yes

**c. Is the information about DOE or contractor employees?**

*This information will be for potential NGP Fellow candidates.*

**2. What is the purpose of the system/application?**

The Nonproliferation Graduate Program (NGP), a National Nuclear Security Administration sponsored program, is a year-long fellowship structured to promote awareness of professional opportunities in nonproliferation and to develop an exceptional talent pool that could aid the National Nuclear Security Administration in its national and international security work. NGP fellows work within NNSA's Office of Defense Nuclear Nonproliferation on programs in support of detecting, preventing, and reversing the proliferation of weapons of mass destruction, while mitigating the risks of nuclear operations.

The purpose of this system is for applicants for the Nonproliferation Graduate Program to fill out an application, upload a resume and letter of interest, and to hold letters of recommendation. Ultimately these pieces of information are used in the selection process. Because of the nature of NGP fellowships, working at NA-20, all selected fellows' job duties will require the handling of information classified up to and including Secret Restricted Data. The individual will also be required to access NNSA security areas and will participate in meetings and interagency working groups involving classified discussions. Therefore all selected participants will be put in for a DOE-Q security clearance and due to the time sensitivity and client needs (all selected fellows holding their security clearance prior to the start of the fellowship in June) the security clearance processing and paperwork requires a streamlined process. For applicants to be vital to NGP, they need to have their information processed immediately after selections in December due to the shorten timeframe (6 months) for which the security clearance needs to be processed and due to the duration of the NGP fellowship (12 months). Thus, it is critical to this program to have individuals fill out a copy of a security clearance questionnaire while applying so that if selected they can instantly replicate the information from the copy on to the SF-86 via E-Quip and the entire security clearance package can be sent to DOE-Chicago for immediate processing.

**3. What legal authority authorizes the purchase or development of this system/application?**

Applications hosted on the server Jomolungma are paid for by DOE, while all development costs are covered by the associated project(s). The NGP Fellow Application System was developed and is operated in accordance with PNNL contract DE-AC05-76RL01830.

**C. DATA IN THE SYSTEM**

**1. What categories of individuals are covered in the system?**

- 1) Applicants seeking an NGP Fellowship appointment.
- 2) PNNL Staff members who process, review, and update application data for the fellowship selection process (hereby known as "NGP Staff").
- 3) NGP Security members (PNNL Personnel security) who will review an applicant's SF-86 form for completeness.

**2. What are the sources of information in the system?**

**a. Is the source of the information from the individual or is it taken from another source?**

Information provided is provided directly by the applicant, with the exception of university transcripts and letters of recommendations. University transcripts, are requested by the applicant, and provided to the NGP office directly by the university. Once received by an NGP staff member, the transcripts are scanned into digital form and uploaded to this online system via an administrative web form in this application restricted by access control.

Requests for Letters of Recommendations (LOR) are initiated by the applicant by providing a name and email address of a requested recommender. The system emails this recommender with a link for completing a LOR for the requesting applicant. Once the LOR form is completed and submitted by the recommender, the information provided is appended to the applicant's records.

SF86 information will be provided directly by the applicant. They will fill out the information in a provided Microsoft word template (.doc) then upload the document to the application server. When submitted, this document will immediately be transferred via notes mail with a secure connection to an intranet server, encrypted then stored in a database with strict ACL controls, allowing only designated NGP Security reviewers access. The information will never be stored on the extranet application server except in memory during the period that the document is transferred internally.

**b. What Federal agencies are providing data for use in the system?**

None.

**c. What tribal, state, and local agencies are providing data for use in the system?**

None.

**d. From what other third party sources will data be collected?**

University transcripts will be acquired directly from the university and letter of recommendations are provided via an online form submission at the request of the applicant.

**e. What information will be collected from the individual and the public?**

The following information will be collected from the user:

1. Full Name
2. If the applicant holds a dual citizenship, and to what countries.
3. Birth city, state and country.
4. Current and permanent address.
5. Primary and alternate email address(es)
6. Emergency contact name, address, and phone number(s)
7. Letter of interest when applying to the NGP program.
8. A current resume, text.
9. SF86 Form data.
10. Information from last six universities, including the following information:
  - a. University name
  - b. Location
  - c. Dates attended
  - d. Academic Major and Minor
  - e. Academic Status
  - f. Degree sought/obtained
  - g. Date degree received.
11. Transcripts provided by each university (scanned / uploaded at a later date)

**3. Accuracy, Timeliness, and Reliability**

**a. How will data collected from sources other than DOE records be verified for accuracy?**

Data provided by the user will be validated during the NGP Fellow selection process. University transcripts will only be accepted directly from the university. Follow-ups may be performed in order to contact those who provided a letter of recommendation, if additional information is required on an applicant. SF-86 information provided by the user will be reviewed by PNNL Personnel security for completeness and accuracy before officially being submitted for review.

**b. How will data be checked for completeness?**

The application process includes server-side completeness validations for all required input provided by the user or recommenders. Applications are automatically reviewed for completeness at each step in the application process by checking the inputted user data for expected data types and formatting. The applicant will be unable to submit the final application unless all pages have been verified as containing expected data by the system. Incomplete items will be enumerated both on the submission page and on each

data entry page a user encounters. Further review for completeness occurs during the application review process by the NGP Staff.

**c. Are the data current? What steps or procedures are taken to ensure the data are current and not out-of-date?**

Data stored in the system will be applicable for the current application cycle only. Archive data will only hold the previous 12 months worth of data. Data older than 12 months will be purged from the system.

**d. Are the data elements described in detail and documented?**

A data dictionary is created and maintained for the system.

**D. ATTRIBUTES OF THE DATA**

**1. Is the use of the data both relevant and necessary to the purpose for which the system is being designed?**

*Yes*

**2. Will the system derive new data or create previously unavailable data about an individual through aggregation from the information collected, and how will this be maintained and filed?**

Applicant transcript information will be uploaded to the NGP application by NGP staff members and related to the applicant's application data via username. Only NGP staff members and server administrators will be allowed access to these transcripts once uploaded. Individual applicants will only see that their transcript(s) and letter of recommendation(s) have been received, but will not be able to access those data items.

**3. Will the new data be placed in the individual's record?**

Yes, transcripts provided by the university and letters of recommendations are appended to the applicant's application. Data will be verified as current by NGP Staff by examining postmark dates on received transcripts and timestamps on letter of recommendations.

**4. Can the system make determinations about employees/the public that would not be possible without the new data?**

*No*

**5. How will the new data be verified for relevance and accuracy?**

Transcript comes directly from the University. Letter of recommendations are followed up on an as-needed basis. SF86 information can only be accessed by designated PNNL Security personnel. Data is reviewed by the aforementioned security staff for correctness and completeness.

**6. If the data are being consolidated, what controls are in place to protect the data from unauthorized access or use?**

Access controls Form-level access controls are applied to uploaded transcripts to prevent those other than NGP staff and Server administrator group members from viewing the data. In the event an unauthorized source attempts to access the data protected by the applied access control, the server will return an Error 404 (File not found).

**7. If processes are being consolidated, do the proper controls remain in place to protect the data and prevent unauthorized access?**

Access Control will always be set at the “document” level, so once the record exists in the system, only users belonging to the role NGP staff can access that data.

**8. How will data be retrieved? Does a personal identifier retrieve the data? If yes, explain, and list the identifiers that will be used to retrieve information on the individual.**

Data (with the exceptions listed below) will be retrieved through a backend database lookup based on an applicant’s username and the data item to be retrieved. This lookup will only be performed from pages where the access control allows such lookup.

Transcript and letter of recommendation data will be retrieved from a database lookup based on the following keys:

- <applicantusername> <transcript filename>
- <applicantusername> <recommender name>

**9. What kinds of reports can be produced on individuals? What will be the use of these reports? Who will have access to them?**

The applicant will be able to visit a “status” page to check what information has been collected for his/her application process. The only data viewable by the user is as YES|NO representation of whether their data has been submitted or received.

NGP Staff members can view a consolidation of the user’s application information, excluding the SF-86 form information.

**10. What opportunities do individuals have to decline to provide information (e.g., where providing information is voluntary) or to consent only to particular uses of the information (other than required or authorized uses)?**

User will check a box stating that their data will only be used for internal purposes for the NGP fellowship program, and will not be shared with 3<sup>rd</sup> parties. A checkbox will be added to record consent, setting a data flag in the user’s “User Info Document” to indicate acceptance. A link will be provided to a page describing why and what the data being collected is being used for.

**E. Maintenance and Administrative Controls**

**1. If the system is operated in more than one site, how will consistent use of the system and data be maintained in all sites?**

This application is hosted on only one site.

**2. What are the retention periods of data in the system?**

The archive database will hold only the previous 12 months of data. All data older than 12 months will be purged from the archive database.

**3. What are the procedures for disposition of the data at the end of the retention period? How long will the reports produced be kept?**

See E.2 above.

**4. Is the system using technologies in ways that DOE has not previously employed (e.g., monitoring software, Smart Cards, Caller-ID)?**

No

**5. How does the use of this technology affect public/employee privacy?**

With the appropriate security measures in place, the privacy impact for the applicant given the data collected is low. The applicant's application and transcript information is intended to only be shared only with those directly affiliated with the NGP Fellowship program. SF-86 form information will only be viewable by designated PNNL Security staff members.

**6. Will this system provide the capability to identify, locate, and monitor individuals?**

No

**7. What kinds of information are collected as a function of the monitoring of individuals?**

N/A

**8. What controls will be used to prevent unauthorized monitoring?**

N/A

**9. Under which PA system of records notice does the system operate?**

"In accordance with clause H-15 of the PNNL contract (DE-AC05-76RL01830), portions of the system collect data that is exported to the system of records DOE-43 "Personnel Security Files". These data are disposed after they are transferred to the Federal Information system of record."

**10. If the system is being modified, will the PA system of records notice require amendment or revision?**

No, the system of record is not being amended or modified.



**F. ACCESS TO DATA**

**1. Who will have access to the data in the system?**

Only NGP staff members and System administrators will have access to the data submitted to this NGP system. PNNL Personnel Security will only have access to the SF86 data provided by the applicant. Transcripts, letters of recommendation and applicant-provided information in this application is accessible via HTTPS to NGP staff members. System administrators may access the data through a lotus notes client. The administrative user must belong to the system administrator group account, be in possession of and use their unique administrative Notes .id file, and provide the correct password for that .id file to identify themselves on the system.

**2. How is access to the data by a user determined?**

Access to the data is based on a unique username and password created by the user.

The user's username is the system's unique identifier for the applicant. It is created when the user creates a system account. They are asked to provide basic information such as name, email, username desired, and password correlating to the username specified. An application password policy dictates the user creates a password with 8+ character and at least one numeric character to prevent efficient brute-force and dictionary attacks against the system.

Any NGP application data created by that user is accessible by only that specific user and NGP staff members. Letters of recommendation and transcript information are not accessible to any applicants, even for the applicant for which the data is attributed. NGP staff members are users that have a valid account on the system and have been added to an appropriate NGP STAFF group by a system administrator. Modifications to individual records will be logged by username and time. Anonymous users are denied access to any information listed above . The system does not use guest accounts.

**3. Will users have access to all data on the system or will the user's access be restricted?**

A user logged into the system with a valid username will have restricted access only to data allowed by access control.

**4. What controls are in place to prevent the misuse (e.g., unauthorized browsing) of data by those having access?**

Access control lists are applied at both the page level and document level for each form where data is entered, and each page where form data is viewed. Audit logs will be used for any modifications made to application data.

**5. Are contractors involved with the design and development of the system and will they be involved with the maintenance of the system? If yes, were PA contract clauses included in their contracts and other regulatory measures addressed?**

Yes, PNNL staff will be involved in the design, development, and maintenance of the system. Individuals provided this access are subject to applicable requirements of the PNNL contract (DE-AC05-76RL01830), internal PNNL operating procedures regarding the protection of sensitive unclassified information and records, and the limitations applicable to DOE officers and employees under the Privacy Act, 5 U.S.C. 552a.

**6. Do other systems share data or have access to the data in the system? If yes, explain.**

The NGP Fellow Application System is leveraging an existing application database for record storage. Page and form level groupname and username based access controls ensure data from one program cannot view data from another program.

Additionally, since SF86 form information will not be stored directly on the external server, this data will be transferred to an intranet server. Access controls will be tightly regulated on the destination database where the SF86 data is stored, preventing anyone except server administrators and authorized PNNL Personnel Security employees.

**7. Who will be responsible for protecting the privacy rights of the public and employees affected by the interface?**

*Jana Fankhauser  
Pacific Northwest National Laboratory  
Global Security Tech & Policy  
Project Manager  
1100 Dexter Ave N. Suite 400  
BSRC  
Seattle, WA 98109-3598  
(206) 528-3264  
Jana.fanhauser@pnl.gov*

**8. Will other agencies share data or have access to the data in this system?**

No.

**9. How will the data be used by the other agency?**


N/A.

10. Who is responsible for assuring proper use of the data?

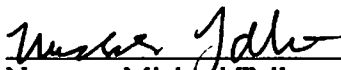
N/A

The following officials have approved this document

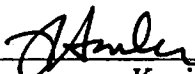
1. System Manager & Owner

 (Signature) 8/11/08 (Date)  
Name: *Jana Fankhauser*  
Title: *Project Manager*

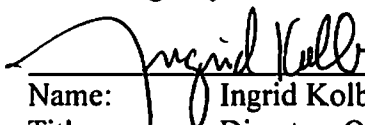
2. Field Privacy Act Officer

 (Signature) 9-15-08 (Date)  
Name: *Michael Talbot*  
Title:

3. Headquarters Privacy Act Officer

 (Signature) 10/16/08 (Date)  
Name: *Kevin F. Hagerty* *JERRY HAWLEY*  
Title: *Director, Office of Information Resources*  
*CHIEF PRIVACY OFFICER*

4. Senior Agency Official for Privacy

 (Signature) 10-24-08 (Date)  
Name: *Ingrid Kolb*  
Title: *Director, Office of Management*

## SIGNATURE PAGE

	Signature	Date
<b>PIA Approval Signatures</b>	<b>Original Copy Signed and On File with the DOE Privacy Office</b>	